NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

North Dakota State and Local Intelligence Center

NDSLIC

1-866-885-8295

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Stolen Fargo mail truck recovered in Grand Forks. Authorities are investigating the theft of a contracted mail truck in Fargo, North Dakota. Police said the truck owned by a private company was parked near a U.S. Postal Service parking building before it was taken late November 4 or early November 5. It was recovered November 5 in Grand Forks.
Source: http://www.thedickinsonpress.com/event/article/id/62732/group/homepage/

Regional

Nothing Significant to Report

National

Nor'easter snow layers Sandy destruction; more evacuations, more power outages. Snow fell on damaged homes and debris piles in parts of the New York City area as a nor'easter moved in, causing new power outages and calls for evacuations, NBC News reported November 8. By November 7, the winds caused more than 100,000 new power outages in the Mid-Atlantic and Northeast, the U.S. Department of Energy stated. That brought the total number of outages to 715,000, most of those remaining from Superstorm Sandy, which made landfall in New Jersey October 29. Throughout the New Jersey, New York, and Connecticut tri-State area, people wore coats indoors as they endured yet another night without heat. About 1,200 flights were canceled across the Northeast, while residents of a few areas hit hardest by Superstorm Sandy were urged to evacuate in case of new flooding. Long Island Rail Road service was also suspended because of weather-related signal problems, WNBC 4 New York reported. The snow from the latest Nor'easter was expected to continue through November 9.
Source: http://usnews.nbcnews.com/_news/2012/11/07/14987947-noreaster-snowlayers-sandy-destruction-more-evacuations-more-power-outages?lite

International

Nothing Significant to Report

Banking and Finance Industry

(New York) **DTCC operations ran during Sandy, vault status still unclear.** The Depository Trust & Clearing Corporation (DTCC) processed about $19 trillion in securities trades the week of October 29 even as Hurricane Sandy submerged its 40-year-old underground Manhattan vault in New York City holding physical stock and bond certificates, Bloomberg News reported November 7. The company switched day-to-day command of its operations to its office in Tampa, Florida, and moved control of the technology that runs its clearing and settlement business and record-keeping to its Dallas data center the weekend before the Atlantic's largest-ever tropical storm, the president and chief executive officer of DTCC, said.

The DTCC handles trades in U.S. equities and government, municipal and corporate bonds, and is more important to how markets function than the New York Stock Exchange or Citigroup Inc., according to a professor at Georgetown University's McDonough School of Business. The DTCC's 10,000-square-foot vault, three levels below ground, contains 1.3 million stock and bond certificates and other securities. The entire 55 Wall Street building remains closed. While the certificates may be damaged if water flowed into the vault, they are already recorded electronically in DTCC's systems, the DTTC CEO said. Once the company can assess the status of the certificates, it will figure out what to do about replacing them, he said. DTCC also has images of all bearer stocks and bonds in the vault, he said.
Source: http://www.businessweek.com/news/2012-11-07/dtcc-operations-ran-duringsandy-vault-status-still-unclear

New Fake Token Android banking Trojan steals logins directly. A new variant of the —Fake Token financial attack on Android devices has targeted customers of several banks in Europe this year, warn security researchers, according to Info security November 2. Unlike other banking Trojans making the rounds, this new threat has no need to first infect PCs to steal bank account passwords. According to analysis by a malware researcher at McAfee Labs, a new version of the Android/Fake Token malware goes back to basics: it is distributed through phishing emails pretending to be sent by the targeted bank. This malware attack simulates the real Internet banking site by asking for confidential information like personal email and phone number, which is then used to initiate the mobile attack. Additionally, unlike previous Trojan bankers for Android such as the first Fake Token version and Zitmo/Spitmo, both authentication factors (Internet password and mTAN)are stolen directly from the mobile device. The trojan also has other means of distribution, including Web page injection and redirects that lead to a fake security app.Source: http://www.infosecurity-magazine.com/view/29134/new-faketoken-androidbanking-trojan-steals-logins-directly/

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(Georgia) **Seven people wounded during shooting at crowded Ga. fair, police say.** Seven people were wounded November 3 when someone opened fire at the crowded Coastal Empire Fair in Savannah, Georgia. Police continued to search for the gunman, who was described as wearing a dark jumpsuit, although investigators have not ruled out the possibility there was more than one shooter. Several people were detained and questioned, but they were all released by investigators. Police announced no arrests November 4 and released no further information on what happened inside the fairgrounds or what motivated the shootings. The police spokesman said the victim believed to be most seriously wounded underwent surgery and was listed in fair condition. None of the injuries were considered life-threatening.
Source: http://www.cbsnews.com/8301-504083_162-57544966-504083/seven-peoplewounded-during-shooting-at-crowded-ga-fair-police-say/

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Master Forge gas grills sold at Lowe's stores recalled due to fire and burn hazards; Made by Guangdong Vanward Electric. The U.S. Consumer Product Safety Commission, in cooperation with Guangdong Vanward Electric, November 6 announced a voluntary recall of about 37,000 Master Forge gas grills. If improperly installed, the hose connecting the gas tank and regulator to the burner control can touch the burner box and cause the hose to melt and rupture when the grill is lit. This poses a fire and burn hazard. Guangdong Vanward is aware of two reports of hoses melting and rupturing. The grills were sold exclusively at Lowe's stores nationwide from November 2011 through May 2012. Consumers should immediately stop using the grill and make sure that the gas hose runs along the outside of the grill cabinet and passes through the round hole in the side panel. Consumers should contact Guangdong Vanward Electric for revised instructions and a warning label to apply to the grill that shows how to properly install the hose and the regulator.
Source: http://www.cpsc.gov/cpscpub/prerel/prhtml13/13028.html

Bose recallsDual-Voltage CineMate II Home Theater Speaker Systems due to fire hazard. TheU.S. Consumer Product Safety Commission, in cooperation with Bose Corporation, November 1 announced a voluntary recall of about 20,500 Dual-Voltage CineMate II Home Theater Speaker Systems. A component in the bass module can fail when used outside of the U.S. in electrical outlets rated at 220 volts or higher, presenting a fire hazard to consumers. Bose received two reports of the bass modules igniting when used in 220-volt electrical outlets in Europe. The systems were sold at U.S. Military Exchanges and select U.S. retailers from September 2009 through September 2012. Consumers were advised to immediately stop using and unplug any dual-voltage CineMate II systems and contact Bose to arrange for a free repair or replacement of the bass module.
Source: http://www.cpsc.gov/cpscpub/prerel/prhtml13/13022.html

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

Nothing Significant to Report

Energy

(California) **800 feet of power lines cut,stolen.** Sometime between October 1 and 20, thieves snipped power lines to steal 800feet of copper valued at $150,000, according to local sheriff's deputies in California'sSanta Clarita Valley, the Santa Clarita Valley Signal reported November 5. Sometimein October, thieves cut the padlock on a gate barring access to property owned by the Department of Water & Power at Oak Avenue, according to a report by deputies of the Santa Clarita Valley Sheriff's Station. Once on the property, the thieves then snipped the power lines between two towers and stole 800 feet of copper wiring, they said. According to an informant, the power lines that were cut were inactive as a result of damage from a large fire 10 years ago. The power lines are attached to multiple towers from Drinkwater Flats to Sun Valley. No arrests were made in connection with the theft.
Source: http://www.the-signal.com/section/36/article/80019/

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

(North Carolina) **Copper thieves delay earlyvoting in Anson County.** Voters in Anson County, North Carolina, had to wait an hour longer to cast their ballots November 3 after copper thieves cut Internet lines at the county's only early voting site. Thieves also stripped 16 air conditioning units of copper at the Anson County Schools administration office in Wadesboro, causing $180,000-$200,000 worth of damage, according to the interim Wadesboro Police chief.
He also said he believes the thieves were not amateurs because of how quickly and efficiently they worked.
Source: http://www.wcnc.com/news/Copper-theft-delays-early-voting-in-Anson-Co-177102941.html

Information Technology and Telecommunications

US-CERT warns of flaws in Symantec products caused by legacy decomposer. The U.S. Computer Emergency Readiness Team (US-CERT) issued an alert regarding a vulnerability in certain Symantec antivirus products, which can be leveraged by a remote attacker to execute arbitrary code with administrative privileges. The issue stems from the fact that some Symantec products fail to properly handle malformed CAB files, resulting in memory corruption. The affected products are Symantec Endpoint Protection 11.0 and Symantec Endpoint Protection Small Business Edition 12.0. These products are impacted because they rely on a legacy decomposer that fails to perform proper bounds check in some specifically formatted files when parsing content to be scanned from the CAB archive. —Successful targeting of this nature would necessarily require the attacker to be able to get their maliciously formatted archive past

established email security policies to be processed on a system. This may lessen the success of any potential attempts of this nature though it does not reduce the severity if successfully executed,   Symantec wrote in its report. The company confirmed that the legacy versions of the decomposer engines can cause crashes when handling malformed CAB files, but they have not been able to verify remote code execution.
Source: http://news.softpedia.com/news/US-CERT-Warns-of-Flaws-in-Symantec-Products-Caused-by-Legacy-Decomposer-305417.shtml

Malware uses password recovery app to extract credentials stored in browser. Most of the pieces of malware designed to steal user credentials, log keystrokes in order to collect the information. However, a new threat called PASSTEAL (TSPY_PASSTEAL.A) relies on a password recovery application to accomplish the task. According to Trend Micro researchers, the malware collects the information stored in Web browser by sniffing out accounts from different online services and apps. The sample analyzed by the security firm contains the PasswordFox app designed to work with Firefox. “In effect, the password recovery tool enables PASSTEAL to acquire all login credentials stored in the browser- even from websites using secured connections (SSL or HTTPS),” a threat response engineer at Trend Micro explained. ”Some sites that use this connection includes Facebook, Twitter, Pinterest, Tumblr, Google, Yahoo, Microsoft, Amazon, EBay, Dropbox, and online banking sites. PASSTEAL also doesn't restrict itself to browser applications. Certain variants are designed to log information from applications such as Steam and JDownloader.” After it extracts the data, the malicious element executes a command to save all the information into a .xml file. Based on this .xml file, a text (.txt) file is also created. Once all the information is gathered, the malware connects to a remote FTP server and uploads the files. Source: http://news.softpedia.com/news/Malware-Uses-Password-Recovery-App-to-Extract-Credentials-Stored-in-Browser-305103.shtml

Agencies join effort to promote use of critical controls for cybersecurity. DHS is launching an initiative to implement automated monitoring of a set of critical security controls in government IT security in 2012, to provide a standardized cybersecurity baseline for agencies, GCN reported November 5. The effort will include a set of technical specifications developed in cooperation with industry that would enable the automation of the controls in off-the-shelf products. There also would be a governmentwide dashboard to provide visibility into each agency’s status on the controls and help establish priorities for improvement during the current fiscal year. The plans were unveiled in conjunction with the November 5 release of the latest version of the top 20 Critical Controls for Effective Cyber Defense and the announcement of a new international organization to oversee development of the consensus controls and promote their use in government and industry. DHS, along with the National Security Agency, the Defense Department, the Defense Information Systems Agency, and the Department of Defense Cyber Crime Center, are among the members of the Consortium for Cybersecurity Action, which will maintain and update the list. Source:
http://gcn.com/articles/2012/11/05/agencies-join-effort-to-promote-critical-controls-for-cybersecurity.aspx

Researchers find smishing vulnerability in Android, all versions affected. Researchers from North Carolina State University identified a smishing vulnerability that affects all versions of Android, including Jelly Bean, Ice Cream Sandwich, Froyo, and Gingerbread. Smishing attacks are phishing attacks that rely on SMS messages. They are often utilized by cybercriminals to steal information from unsuspecting mobile phone users. According to an associate professor at the university's Department of Computer Science, the security hole can be leveraged by an application to create fake arbitrary SMS messages. —One serious aspect of the vulnerability is that it does not require the (exploiting) app to request any permission to launch the attack (In other words, this can be characterized as a WRITE_SMS capability leak.), he explained. Google was informed of the vulnerability. The company promised to address the issue in a future Android release.
Source: http://news.softpedia.com/news/Researchers-Find-Smishing-Vulnerability-in-Android-All-Versions-Affected-Video-304464.shtml

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

"USPS delivery problem" spam leads to malware. Help Net Security reported November 6 that fake emails seemingly coming from U.S. Postal Service (USPS) telling customers that they have failed to deliver packages on time actually contain a downloader trojan. Hoax-Slayer warned that the USPS logo, delivery bar code, and shipping numbers make the spoofed notification look rather legitimate. However, the link that supposedly takes users to a printable shipping label with instructions to take it to the nearest "UPS" office will actually lead users to a compromised Web site that will automatically download a file named Shipping_Label_USPS.zip. At the time when the spam campaign was first spotted the Trojan had an extremely low detection rate.
Source: http://www.net-security.org/malware_news.php?id=2310

Public Health

(Tennessee) **Meningitis outbreak: TN reports 13th death.** A thirteenth death from fungal meningitis was reported in Tennessee, the Centers for Disease Control and Prevention (CDC) said November 5. The number of Tennessee illnesses grew by 1 to 79, the State health department said. The additional case of sickness was not included in the CDC's count. Tennessee's additional case of infection brings the national tally to 420, including 10 joint infections. All are associated with potentially contaminated epidural steroid injections from the New England Compounding Center, a specialty pharmacy in Framingham, Massachusetts. Michigan leads the nation with 119 reported cases, 7 more than what was reported November 2. New meningitis cases also were reported in Indiana, New Hampshire, New Jersey, and Virginia the weekend of November 3, the CDC said. New Hampshire also reported a new joint infection, its fourth.
Source:

http://www.tennessean.com/article/20121105/NEWS07/311050049/Meningitisoutbreak-TN-reports-13th-death

Transportation

(Michigan) **Mich. shootings spree suspect arraigned, jailed.** A man suspected in two dozen random shootings along a 100-mile stretch of roadway in southeastern Michigan was charged with several gun crimes November 7 that were likely the first of many charges. The shootings occurred in four counties — Ingham, Oakland, Livingston, and Shiawassee — between October 16 and October 27. Prosecutors believe that the suspect is responsible for the shootings in October that mostly targeted moving vehicles or occurred near Interstate 96. One person was injured. The alleged shooter was ordered held on a $2 million bail after being charged with assault with a dangerous weapon and other gun crimes. The chargesstem from a shooting October 18 on an Interstate in Livingston County's Howell Township, about 45 miles northwest of Detroit. Source: http://www.nytimes.com/aponline/2012/11/07/us/ap-us-michigan-shootingspree.html?

Water and Dams

Nothing Significant to Report

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168